International Journal of Engineering & Technology, 7 (4) (2018) 2541-2545

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.14744
Research paper

Methods and models of protecting computer networks from unwanted network traffic

Gulomov Sherzod Rajaboevich [1] *, Ganiev Abdukhalil Abdujalilovich [1]

[1] *Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan*
**Corresponding author E-mail: sherhisor30@gmail.com*

Abstract

In this article a method of measure network traffic to collect data about the header of packets and to analyze the traffic dump in computer networks are offered. A method for detecting anomalies and a formal model for protecting information from DDoS attacks, which make it possible to simplify the development of filter rule sets and improve the efficiency of computer networks, taking into account, the interaction of detection modules and the use of formal set-theoretic constructions are proposed.

Keywords: *TCP SYN Flood; Ping of Death; Tribe Flood Network (TFN); Stacheldraht; IP Spoofing.*

1. Introduction

Currently, the basic concepts of cyber security are accessibility, integrity and confidentiality. Distributed Denial of Service (DDoS) attacks affects the availability of information resources. DDoS is considered successful if it has led to inaccessibility of the information resource. The success of the attack and the impact on the target resources are different in that the impact damages the victim.

There are several methods for increasing the power of DDoS attacks, but the basic idea is almost the same. The attacker performs IP spoofing and sends fake requests to the vulnerable UDP-server. Not knowing that the requests are fakes, the server is preparing a response. The problem occurs when the server sends thousands of replies to the attacked host, thereby causing its denial of service. Attacks using the enhancement methods are very effective, since the size of the response packets exceeds the size of the request packets. As a result, an attacker, even with insignificant resources, can implement a powerful DDoS attack. Researchers regularly record such attacks, but new previously unknown methods, cybercriminals use extremely rarely. This includes, in particular, the Memcrashed attack, which involves augmenting the attack using memcached UDP. In recent days, the number of attacks Memcrashed began to grow rapidly.

2. Hierarchy of processes for measuring network traffic

The measurement of network traffic consists of two phases: data acquisition and analysis.

At the first phase, a procedure is performed for the direct measurement of traffic characteristics. Data collection is carried out at any point of the network by tools that register packet traffic, with information on the packet headers and the time stamp for their registration.

At the second phase, the processing of the collected information is carried out using tools that allow you to convert data according to the models used and provide traffic characteristics in the form of numerical values or initial data for plotting.

Tools, used during the measurement: a utility for capturing IP packets on the network interface - creating a traffic dump, a dump analysis utility, a graphing utility.

The measurement objects can be physical signals in a transmission channel, individual packets, and virtual connections consisting of sequence packets and aggregated traffic [1]. When taking measurements, the following important factors should be considered:

- Each dimension changes the state of the packet. When a packet passes through an intermediate network device, the Time to Live (TTL) is reduced by one and the checksum is recalculated for each packet;
- Packet measurement "disturbs the network". There is an addition of delays in the process of transferring packets, which in turn leads to the appearance of new properties;
- Measured traffic characteristics can be obtained on the time interval that is associated with the minimum packet size and the lifetime of the virtual TCP connection.

To estimate the measurements of network traffic, it used the throughput of the network of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi and the length of the packet. In the results of the experiment, it was determined that the throughput of the network of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi is
100 Mbit/s. Estimates of network traffic measurements are denoted by the formula:

$$\Delta t = \frac{l_p}{\lambda} \quad (1)$$

Where
l_p – Length of the packet;
λ – Channel throughput.

In Table 1 is shown the results of estimates of network traffic measurements in different channel throughput and the length of the packets.

Table 1: Estimates of Network Traffic Measurements in Different Channel Throughput and Length of the Packet

№	length of the packet l_p (minimum)	length of the packet l_p (long)	length of the packet l_p (higher long)	Throughput λ	Estimates of network traffic measurements for the minimum packet $\Delta t = \frac{l_p}{\lambda}$	Estimates of network traffic measurements for a long packet $\Delta t = \frac{l_p}{\lambda}$	Estimates of network traffic measurements for a higher long packet $\Delta t = \frac{l_p}{\lambda}$
1	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	10 Mbit/s	0,000048=48× 10^{-6} Mbit/s	0,0011=11× 10^{-4} Mbit/s	00,0045=45 ×10^{-4} Mbit/s
2	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	50 Mbit/s	0.0000096 = 96 × 10^{-7} Mbit/s	0,00022 = 22 × 10^{-5} Mbit/s	0,0009=9×10^{-4} Mbit/s
3	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	100 Mbit/s	0.0000048 = 48 × 10^{-7} Mbit/s	0.00011 = 11 × 10^{-5} Mbit/s	0,00045=45× 10^{-5} Mbit/s
4	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	1000 Mbit/s	0.00000048=48 × 10^{-8} Mbit/s	0.000011 = 11 × 10^{-6} Mbit/s	0,000045=45× 10^{-6} Mbit/s
5	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	5000 Mbit/s	0.000000096 = 96 ×10^{-9} Mbit/s	0.0000022 = 22×10^{-7} Mbps	0.000009 =9× 10^{-6} Mbit/s
6	64 bytes = 0.00048 Mbit	1500 bytes = 0.011 Mbit	6000 bytes = 0.045 Mbit	10,000 Mbit/s	0.000000048 = 48×10^{-9} Mbit/s	0.0000011 = 11×10^{-7} Mbit/s	0,0000045= 45×10^{-7} Mbit/s

It should be noted that measuring the characteristics of network traffic makes it possible to collect information about packet headers and provide a packet in the form of numeric values, which allows to detect packets and analyze the traffic dump at any point on the network.

3. Method for detecting anomalies in the network traffic

Causes and sources of anomalies in the network traffic. There are visible anomalies, manifested in the incorrect operation of the system at the current time and anomalies that have no visible signs at the current time, but which can lead to failures after a considerable time. At the same time, the more dangerous are the anomalies that arise as a result of the DoS attack.

In Table 2 is described the various and consequences of anomalies in network traffic.

Table 2: The Causes and Consequences of Anomalies in the Network Traffic

The cause of the anomalies	Type of manifestation of anomalies	Consequences
Application-level attacks	Exploitation of known vulnerabilities and errors in the software, scanning and access to ports associated with vulnerable applications.	Attackers can access the network, increase privileges, and gain administrative access.
Auto router	Traffic jumps on flows	Installing rootkit and using the system to automate the intrusion process, allows an attacker to scan hundreds of thousands of systems in a short time
DoS and DDoS attacks	There is an intense traffic flow from multiple IP addresses to the ports of routers and servers	There are violations of the normal functioning of the system, the availability of data and services is disrupted, which are usually supplemented by a lack of resources necessary for the network, operating system or applications
TCP SYN Flood	Creating a large number of partially open connections, increasing the number of SYN packets	Violations of the normal functioning of the system
Ping of death attacks	Getting too large IP packets	Failure, refusal, freezing and rebooting the system
Tribe Flood Network (TFN) and Tribe Flood Network (TFN2K)	Generating packets with spoofed source IP addresses, dynamically changing the size of packets, IP addresses and source ports, the appearance in traffic of a large number of packets per IP address	They are distributed tools, usually launching coordinated DoS attacks from many sources for one or more purposes
Stacheldraht	The appearance of illegal encrypted traffic generation of packets with spoofed source IP-addresses, dynamically changing the size of packets	There is an invasion of a large number of systems for their subsequent use in an attack.
IP spoofing attacks	Substitution of source IP addresses with addresses from trusted zones	An intruder inside or outside the network pretends to be a computer you can trust
"Man-in-the-middle" attacks	Interception of network packets, routing protocols and transport protocols, distortion of transmitted data and inclusion of new information in network sessions	Information theft, hacking of the current session to gain access to private network resources, traffic analysis - to obtain information about the network and its users, DoS attacks, distortion of transmitted data and the inclusion of new information
Network intelligence	Requests for the DNS server, scanning for the range of IP addresses and port scanning.	Attackers can find open ports, examine the characteristics of applications running on hosts.
Packet sniffing	Intercepting packets transmitted over the network in an open manner (Telnet, FTP, SMTP, POP3, etc.), such as user names and passwords, switching traffic flows from one network device to another	An attacker can access a system user account.
Port forwarding attacks	Redirects network traffic, dropping in bytes or packets in a single traffic flow.	Passing Illegal traffic via firewall by Intruders
Attacks on the	Occur when someone takes advantage of the trust	Attack in the internal network

exploitation of confidential property	relationship within the network

A large number of rules in the set of the problem of detecting anomalies may require time resources, there is also the possibility that the specialist who is solving this problem can miss an error or, conversely, calculate for an error that is not so.

To solve the above problems, a method for detecting anomalies in the network traffic is proposed [2-3]. The main differences between the proposed method and existing ones is that the proposed method not only detects anomalies in sets of filtering rules, but simplifies the process of developing sets of filtering rules. The implementation of the proposed method consists of consistently executing the following modules:

- module for interception of the network traffic;
- module for generating formal rules;
- module of parsing network packet.

In Figure 1 is presented the interaction stages of the anomaly detection modules in the network traffic.

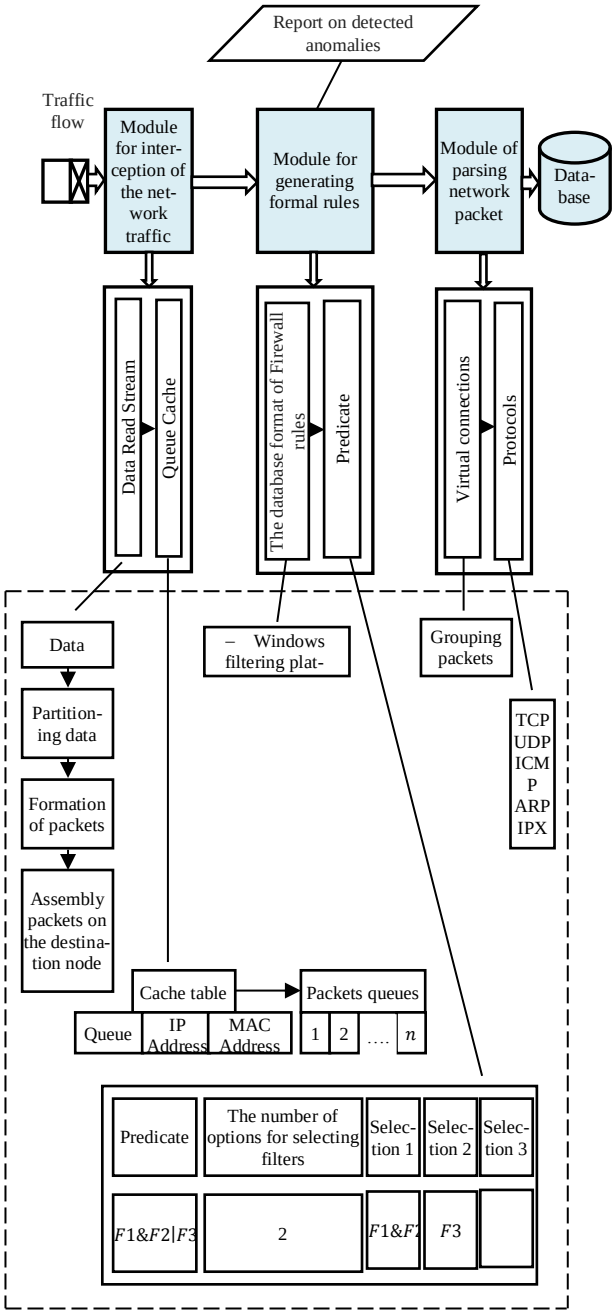

Fig. 1: The Interaction Stages of the Anomaly Detection Modules.

Module for interception of the network traffic. Packets, intercepted by the module for interception of the network traffic are input to the module for generating formal rules. Then the packets are transformed into a module for generating formal rules, that is, rules that are not tied to a particular Firewall model.

Module for generating formal rules. In the process of transformation to the formal form of rules, information is used from the library describing the formats of Firewall rules. The format of the Firewall rules is an XML file containing a scheme for converting formal rules into the format of a particular Firewall. For a number of Firewall that have the binary format of a set of filter rules and do not offer the possibility of exporting / importing it into a text format, the description database may contain not just XML files for conversion schemes, but a library of functions that allow to convert the binary format of the rule set to text and on the contrary. In the event that the required Firewall is not in the list of supported by the system, the user has the ability to create XML files and conversion libraries independently. Then, the filter rules are distributed among a number of filters:

If the rule is permissive, it will be added to each filter.

If the rule is prohibitive, then for a consistent chain of filters, one rule is sufficient and for parallel filter chains, it is sufficient that the rule be applied to one filter from each chain.

If the rule is prohibitive, then it is necessary to determine the forms of the filter predicate.

For filters in one chain, the rule is applied to any of the filters, and here filters are written in the predicate via OR (|).For filters in parallel chains, a rule is applied to each of them and here filters are written in the predicate via AND (&).The resulting set of formal rules is analyzed and a report on the detected anomalies is then generated.

Module of parsing network packet. In the module of parsing network packet virtual connections are performed. At the end of each of the virtual connections, the source and destination IP addresses, the source and destination ports, the amount of transmitted / received traffic to the database are stored. The only exceptions are ICMP and ARP packets - data about them are stored in the database without aggregation of virtual connections. The database is implemented using SQL-queries, which allows you to take full advantage of all the features and flexibility of the SQL language. By creating the necessary queries to the database, you can get all the necessary information to build a set of filter rules to the point of interception of the analyzed network traffic.

4. A formal model for protecting network traffic from DDOS attacks

Classification of DDoS-attacks. This is a simplified classification by protocols and by the mechanism of action used to transmit data in computer networks [4-5], the vulnerabilities of which are used by hackers, organizing attacks. In Table 3 is given the classification of DDoS attacks in the computer networks.

In Table 4 is presented DDoS-attacks are possible on each of the seven levels.

Table 3: Classification of DDOS Attacks in the Computer Networks

By protocols	On the mechanism of action

	The first group is attacks aimed at overflowing the communication channel, in other words, various types of flooding.	The second group which has fewer types of denial-of-service attacks, are attacks that exploit the network protocol stack vulnerability	The third group is DDoS attacks on the application layer
TCP HTTP UDP ICMP	1) DNS amplification 2) Fragmented UDP flood 3) ICMP flood 4) NTP amplification 5) NTP flood 6) Fragmented ACK flood 7) Ping flood 8) UDP flood 9) UDP-flood using a botnet 10) VoIP flood 11) Flood with media data 12) Attack with ICMP ECHO broadcast packets 13) Attack with broadcast UDP packets 14) Fragmented ICMP flood 15) DNS flood 16) 16. Other attacks with amplification (amplification)	1) SYN Flood 2) 2. IP null attack 3) 3. Attack of fake TCP sessions 4) TCP null attack 5) Attacks with modification of the TOS field 6) ACK / PUSH ACK flood 7) RST / FIN flood 8) SYN-ACK flood 9) TCP null / IP null attack 10) Attack of fake TCP sessions with multiple SYN-ACKs 11) Attack with the substitution of the address of the sender with the address of the recipient 12) Attack with redirection of traffic of high-loaded services 13) Attack of fake TCP sessions with multiple ACKs	1) HTTP flood 2) Application failure attack 3) HTTP flood with single requests 4) Attack with fragmented HTTP packets 5) HTTP flooding with single sessions 6) Session attack. Attack with slow sessions

Table 4: Comparative Analysis of Possible Attacks on the OSI Model

OSI model		Examples of DDoS technologies	Consequences of DDoS attack
7	Application layer	PDF GET requests, HTTP GET, HTTP POST, HTTP flood, Slowloris Attack (web site forms: login, photo / video upload, feedback confirmation)	Lack of resources. Excessive consumption of system resources by services on the attacked server.
6	Presentation layer	Underlying SSL requests: checking encrypted SSL packages is very resource intensive, attackers use SSL for HTTP attacks on the victim server	Attacked systems may stop accepting SSL connections or automatically rebooting
5	Session layer	The attack on the Telnet protocol uses the weak points of the Telnet server software on the switch, making the server inaccessible	It makes it impossible for the administrator to control the switch
4	Transport layer	SYN-flood, Smurf-attack (attack ICMP-requests with changed addresses)	Reaching the limits of the width of the channel or the number of permissible connections, disruption of the network equipment
3	Network layer	ICICMP flood - DDoS attacks on the third layer of the OSI model, which use ICMP messages to overload the bandwidth of the target network	Reducing the throughput of the attacked network and the possible congestion of the firewall
2	Data link layer	MAC-flood - overflow with data packets of network switches	Data flows from the sender to the recipient block all ports
1	Physical layer	Physical destruction, physical disruption to work or management of physical network assets	Network equipment is unusable and needs repair to resume work

The formal model of information of protection from DDoS attacks is described using formal set-theoretic constructions [6-7].
Let's imagine a model of information protection from DDoS attacks in the form of a tuple:

$$M =< IP, OP, HN, HC, IA, U > \quad (2)$$

Where
IP – Incoming packets;
OP – Outgoing packets;
HN – A set of nodes (hosts) of the computer network
HC – Set of connections between nodes of the computer network
IA – Scenario of the implementation of the attack;
U – A parameter characterizing the user's actions.
Figure 2 shows a formal model of information of protection from DDoS attacks.

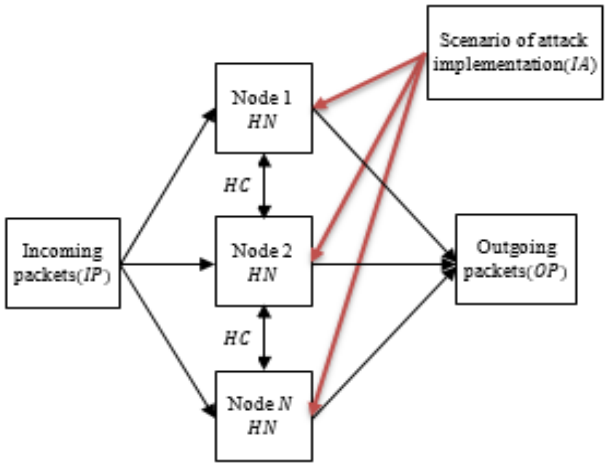

Fig.2: Formal Model of Information Protection from DDOS Attacks.

The set of HN nodes is given in the form of a tuple of elements:

$$HN =< Equipment, Role, Software, Hardware, Function >$$

Where
$Equipment$ – Multiple types of equipment corresponding to the node of the computer network;
$Role$ – Set of functional roles of the node;
$Software$ – A variety of software components used by the nodes;
$Hardware$ – A set of hardware components used by the nodes;

$Function$: $Role \rightarrow Software -$ function that implements mapping of the set of functional roles of a node to a set of software components.
The software and / or hardware component of the software is a protocol that implements a set of rules and allows for the connection and exchange of data between two or more devices included in the network.
The set of HC links between the nodes of the computer network in the context of various protocols is described as follows: it is assumed that the nodes $1,2,\dots N$ of the network are connected by some protocol if there is at least one non-empty finite sequence with the initial node 1 and the end node 2 through which will be a message.
The scenario for implementing the attack contains:

$$IA =< FA_{fuction\ attack}, AA_{against\ attack}, LA_{legitimate\ activities}, WAA_{warning\ about\ attack}, RTA_{response\ to\ attack} > \quad (3)$$

Where
$FA_{fuction\ attack} -$ The functioning of the DDoS attack;
$AA_{against\ attack} -$ Deterrence of DDoS attacks and counteracting attacks;
$LA_{legitimate\ activities} -$ Legitimate activity of the computer network;
$WAA_{lwarning\ about\ attack} -$ Warning about DDOS attacks
$RTA_{response\ to\ attack} -$ Response to DDOS attacks.
In this case, each intermediate scenario becomes the object of subsequent decomposition.
Scenarios $FA_{fuction\ attack}$ contain sub-scenarios for the spread of the DDoS attack, its management and the implementation of attacks.
Scenarios $AA_{against\ attack}$ contain sub-scenarios to counteract the spread of DDoS attacks, counteracting its management and countering the implementation of attacks.
Scenarios $LA_{legitimate\ activities}$ are designed to generate legitimate traffic patterns.
Scenarios $WAA_{lwarning\ about\ attack}$ are designed to mitigate the consequences of an attack on a victim.
Scenarios $RTA_{response\ to\ attack}$ are designed to detect and respond to DDoS attacks.

5. Conclusion

Because of the measuring network traffic experiment, it was revealed that for packet interception and traffic dump analysis it is necessary to consider the size, length and delay of packets and decrease the lifetime of the virtual TCP connection for each packet. With the analysis of the traffic dump, a method for detecting anomalies in the network traffic has been developed, which makes it possible to reduce information security risks with improperly configured rules and reduce the number of network anomalies of filtering rules in the computer networks. Based on the method for detecting anomalies in the network traffic, a formal model for protecting network traffic from DDoS attacks is proposed, which allows more efficient protection of networks from unauthorized traffic.

References

[1] LinY-D., LuCh-N., LaiY- Ch., etal. Application classification using packet size distribution and port association // J. Network Computer Appl. 2009. V.32. – P.1023-1030.
[2] Gulomov Sh.R. Rakhmanova G.S., Boymurodov B.E. Ensuring Secure Info-Communication Networks Based on the Special Filtering Mode. International Journal of Engineering Innovation & Research. Volume 5, Issue 1, 2016, ISSN: 2277 – 5668, India, -P.16-23.
[3] William Stallings. Network security essentials: Applications and Standards Fourth edition. Prentice Hall, USA, 2011. – P.417.
[4] Behrouz A. Forouzan. Data Communications and Networking.5th Edition / McGraw-Hill Forouzan series, New-York USA, 2007. – P.1134.
[5] William Stallings. Data and Computer Communications (10th Edition). International Edition, 2013. – P.912.
[6] D. van Dalen: Logic and Structure (fourth extended ed. Revised). (Springer Verlag, Berlin, 2008).
[7] M. Rathjen: Metamathematical Properties of Intuitionistic Set Theories with Choice Principles. In: S.B. Cooper, B.Lowe, A.Sorbi (eds.): New Computational Paradigms: Changing Conceptions of What is Computable (Springer, New York, 2008) P.287-312. https://doi.org/10.1007/978-0-387-68546-5_13.